

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF RHODE ISLAND

UNITED STATES OF AMERICA

v.

JORDAN MONROE,

Defendant.

Criminal Case No. 16-55-S

GOVERNMENT'S RESPONSE TO DEFENDANT'S
MOTION TO SUPPRESS § 2703(d) ORDERS

Defendant Jordan Monroe's Motion to Suppress should be denied because: (1) the § 2703(d) orders were issued by a court of competent jurisdiction; (2) there is no suppression remedy for alleged violations of §2703(d); (3) the sole case on which the motion relies is both distinguishable and wrongly decided; and (4) the good faith exception applies. Each are independent grounds for denying the motion to suppress.

FACTS

In May 2016, agents from the Department of Homeland Security, Homeland Security Investigations ("HSI"), with assistance from the Rhode Island Internet Crimes Against Children Task Force ("ICAC") executed a federal search warrant at the defendant's residence on Jambray Avenue in Warwick, RI. Execution of the search warrant revealed that the defendant maintained an enormous cache of child pornography on a server he built, including child pornography he produced himself. The defendant was subsequently indicted on six counts of production of child

pornography, two counts of receipt of child pornography and one count of possession of child pornography.

The search warrant was issued by a United States Magistrate Judge for the District of Rhode Island. The statement of probable cause in the affidavit supporting the search warrant application included, among other facts, reference to two Orders (“the Orders”) issued by a United States Magistrate Judge for the District of Columbia pursuant to 18 U.S.C. § 2703. Both Orders directed a third party electronic service provider¹ to produce business records which included the dates, times and IP addresses relating to a list of unique URLs which contained files that depicted child pornography. The child pornography files had been identified and downloaded at the Department of Justice, Child Exploitation and Obscenity Section, High Technology Investigative Unit (“CEOS-HTIU”), located in Washington, DC. CEOS-HTIU was investigating an internet Bulletin Board (“Bulletin Board A”) located on “The Onion Router” or “Tor,” which is a network for anonymous communication designed to conceal the location and identity of users from law enforcement. Bulletin Board A provided URL links to child pornography files on the FSS. See Ex C- Search Warrant Affidavit at ¶6-11.²

The records produced in response to the Orders included IP addresses used to download child pornography in October and December 2015. Through further

¹ To protect the integrity of the investigation, the file sharing service was identified in the affidavit as “FSS.”

² Defendant’s Motion to Suppress contains all exhibits cited herein. Accordingly, this response cites to those exhibits rather than recreate duplicates.

investigation, law enforcement was again able to link the IP addresses to the defendant's residence, and subsequently applied for the residential search warrant. Id.

ARGUMENT

1. The Magistrate Judge had jurisdiction to issue the §2703(d) Orders

The United States Magistrate Judge in the District of Columbia that issued both §2703(d) orders was a "court of competent jurisdiction" for purposes of the Stored Communications Act ("SCA") 18 U.S.C. § 2701 et seq., because it had territorial jurisdiction over the offense being investigated: the distribution of child pornography and related offenses. Child pornography files from FSS, which were accessed from URLs located on Bulletin Board A were downloaded at CEOS-HTIU, located in the District of Columbia. (Ex C at ¶10-11). Venue and territorial jurisdiction for child pornography offenses lies in any district from, through or into which the child pornography moves. See United States v. Cameron, 733 F.Supp 2d. 177 (D.ME 2010). Thus, the offense being investigated (distribution of child pornography) occurred, at least in part, in the District of Columbia and the Magistrate Judge had territorial jurisdiction. Accordingly, the Orders were valid.

While it is true that the Applications for the Orders did not detail the factual basis for territorial jurisdiction in the District of Columbia, there was in fact territorial jurisdiction and in both applications, the applicant Attorney for the United States advised the Court that it was "a court of competent jurisdiction." Ex A-1 and B-1 at ¶2. Furthermore, both applications asserted "Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated." Id. The plain

meaning of the assertion is that an offense being investigated occurred, at least in part, in the District of Columbia. In determining its own jurisdiction, the Court was entitled to rely on that representation by the attorney for the government, an officer of the Court. Defendant does not point to, nor has the government found, any authority that suggests otherwise.

2. Suppression Is Not A Remedy For Stored Communications Act Violations

Section 2708 of the Stored Communications Act expressly states:

The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.

18 U.S.C. § 2708.

The “remedies and sanctions described in this chapter” include criminal prosecution (18 U.S.C. § 7201) and civil damages (18 U.S.C. § 7207). Suppression is not among the available remedies. Thus, even if the defendant was correct that the Orders were in some way deficient, the statute expressly prohibits suppression as a remedy:

Statutory violations of the SCA, without more, are not remedied through exclusion of the resulting evidence in court. The text of the SCA itself states that ‘[t]he remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.’ The SCA’s enumerated remedies do not include suppression, and numerous courts have held that defendants claiming only statutory violations of the SCA are not entitled to exclusion of the collected evidence.

United States v. Gaspirini, 2017 WL 3038227 (E.D.NY, 2017). See also e.g., United States v. Smith, 155 F.3d 1051, 1056 (9th Cir.1998) (“the Stored Communications Act does not provide an exclusion remedy. It allows for civil damages ... and criminal punishment ... but nothing more.”); United States v. Guerrero, 768 F.3d 351, 358 (5th

Cir. 2014); United States v. Powell, 444 Fed.Appx. 517, 520 (3d Cir. 2011); United States v. Scully, 108 F. Supp. 3d 59, 88 (E.D.N.Y. 2015) (collecting cases); United States v. Stegemann, 40 F.Supp.3d 249, 271 (N.D.NY 2014).

Monroe does not address this provision of the SCA. He also does not allege a constitutional violation, nor can he. The challenged §2703(d) Orders did not order the disclosure of the *content* of any electronic communications, and no content was provided. Rather, the Orders merely required the disclosure of business records of FSS: dates, times and IP addresses that accessed particular URLs. There is no Fourth Amendment expectation of privacy in such records. “Myriad authorities affirm that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation.” United States v. Morel, 2017 WL 1376363 (D. NH 2017), citing United States v. Perrine, 518 F.3d 1196, 1204-05 (10th Cir. 2008) (collecting cases). “Such subscriber information includes, among other things, a subscriber's name, address, and IP address.” Id. See also United States v. D'Andrea, 497 F.Supp.2d 117, 120 (D.MA 2007) (“federal courts [have] uniformly conclude[d] that internet users have no reasonable expectation of privacy in their subscriber information, the length of their stored files, and other noncontent data to which service providers must have access.”). “An IP address provides only the location at which one of any number of computer devices may be deployed, much like a telephone number can be used for any number of telephones.” Combat Zone Inc. v. Does 1-84, 2013 WL 1092132 (D.MA 2013), citing In re BitTorrent Adult Film Copyright Infringement Cases, 296 F.R.D. 80, 84 (E.D.NY 2012). For decades, Courts have consistently concluded that individuals lack a reasonable

expectation of privacy in telephone records. See e.g., Smith v. Maryland, 442 U.S. 735, 745 (1979).

As the Supreme Court has explained, “only defendants whose Fourth Amendment rights have been violated” should be permitted “to benefit from the [exclusionary] rule's protections.” Rakas v. Illinois, 439 U.S. 128, 134 (1978). Monroe’s Fourth Amendment rights were not implicated, let alone violated; therefore suppression is prohibited by the plain language of the SCA at § 7208.

3. Defendant’s reliance on Levin is misplaced

Monroe’s claim relies entirely on the reasoning in United States v. Levin, 186 F.Supp 3d. 26 (D. MA 2016)(presently on appeal, First Circuit Court of Appeals Docket No. 16-1567). In Levin, the FBI obtained a search warrant to deploy a Network Investigative Technique (“NIT”)—a set of computer instructions designed to transmit computer-related identifying information, including the actual IP address, from the computers (wherever located) of users of a child pornography website back to a government-controlled computer—to locate and identify individuals who had accessed the website to view and share child pornography (the “NIT warrant”). The District Court suppressed evidence obtained as fruits of the search under the theory that the NIT warrant was *void ab initio* and not subject to the good faith exception to the exclusionary rule.

Levin is factually distinguishable because it involved an alleged claim of an unconstitutional search of an individual’s computer rather than a statutory claim

regarding third party business records. Thus, even if Levin were correctly decided, it would not govern here.

In any event, the government's position is that Levin was wrongly decided. See generally, Government's Opening Brief in United States v. Alex Levin, Appeal No. 16-1567, United States Court of Appeals for the First Circuit. As Monroe admits, Levin is a minority view. (Motion to Suppress at ¶16 "Judge Young's decision is admittedly the minority view on this issue."). In fact, approximately fifty federal courts have denied or recommended denying suppression resulting from the NIT warrant at issue, and only five, including the District Court in Levin, granted or recommended granting suppression. See Citation of Supplemental Authorities Pursuant to Fed. R. App. 28(j) filed May 5, 2017 by the United States in Levin. Of those five cases where suppression was granted or recommended, Levin is actually the only decision that stands, for now. See United States v. Horton, --- F. 3d. ---, 2017 WL 3122073 (8th Cir. Jul. 24, 2017) (finding magistrate lacked jurisdiction to issue NIT warrant which resulted in constitutional violation, but suppression inappropriate under Leon "good faith" exception); United States v. Workman, --- F. 3d. ---, 2017 WL 3092174 (10th Cir. Jul. 21, 2017) (assuming for purposes of argument that magistrate lacked jurisdiction to issue NIT warrant which resulted in constitutional violation, suppression inappropriate under Leon "good faith" exception). United States v. Carlson 2017 WL 153995 (D.MN, 8th Circuit) is a magistrate's report and recommendation that has yet to be adopted, and its conclusion has been abridged by Horton; United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016) was not appealed but is in the 10th Circuit and therefore abridged by Workman.

4. The good faith exception applies

Even if the Court finds the Orders were invalid notwithstanding the above, suppression is not a permissible remedy for a separate reason: it would not be appropriate under the good faith exception to the exclusionary rule.

The good-faith exception to the exclusionary rule articulated in United States v. Leon, 468 U.S. 897 (1984) makes clear that when police act in “objectively reasonable reliance on a subsequently invalidated search warrant” obtained from a neutral and detached magistrate, “the marginal or nonexistent benefits produced by suppressing evidence . . . cannot justify the substantial costs of exclusion.” 468 U.S. at 922. Monroe does not even allege a lack of good faith. The good-faith exception thus recognizes that where, as here, “an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope . . . there is no police illegality and thus nothing to deter.” Id. at 920-21.

Supreme Court precedent dictates that suppression is a remedy of last resort, to be used for the sole purpose of deterring future Fourth Amendment violations, and only when the deterrence benefits of suppression outweigh its heavy costs. Davis v. United States, 564 U.S. 229, 237 (2011); Herring v. United States, 555 U.S. 135, 140-41 (2009). “The fact that a Fourth Amendment violation occurred—*i.e.*, that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rule applies.” Id. (citing Illinois v. Gates, 462 U.S. 213, 223 (1983)). “To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can

meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system.” Herring, 555 U.S. at 144.

Herring, for example, invoked the good-faith exception in a case involving the arrest of an individual pursuant to a rescinded, and therefore non-existent, arrest warrant. The Supreme Court held that suppression was inappropriate where “an officer reasonably believes there is an outstanding arrest warrant, but that belief turns out to be wrong,” even though the error was due to police negligence. 555 U.S. at 137. Arizona v. Evans, 514 U.S. 1, 15-16 (1995) was another case involving the arrest of an individual pursuant to a quashed, and therefore non-existent, warrant. The Court held that the arresting officer had acted “objectively reasonably when he relied upon the police computer record,” which contained an error made by a court clerk, and that “the Leon framework supports a categorical exception to the exclusionary rule for clerical errors of court employees.” In Davis, the Court invoked the good-faith exception in a case involving the warrantless search of a car’s driver incident to his arrest pursuant to binding legal precedent later overruled, 564 U.S. at 241. In Illinois v. Krull, 480 U.S. 340, 354-57 (1987), the Court invoked the good-faith exception in a case involving the warrantless search of a junkyard pursuant to a state statute later declared unconstitutional. In all of those cases, the Supreme Court found that the warrantless search or arrest at issue violated the Fourth Amendment, and yet the Court found suppression inappropriate because law enforcement had acted in objectively reasonable reliance on the subsequently invalidated warrant, statute, or

legal precedent that would have authorized the search or arrest, and exclusion therefore would not deter future police misconduct.

Assuming, arguendo, that the 2703(d) Orders were void because the magistrate judge lacked territorial authority to issue them, and further assuming that the CEOS-HTIU's obtaining the FSS' business records thereby amounted to an unconstitutional warrantless search or was otherwise somehow invalid, suppression is not warranted because the agents acted in objectively reasonable reliance on the subsequently invalidated Orders and were in no way culpable for the D.C. Magistrate Judge's purported error. See Davis, 564 U.S. at 240 (noting that, "in 27 years of practice under Leon's good-faith exception, we have never applied the exclusionary rule to suppress evidence obtained as a result of nonculpable, innocent police conduct") (internal quotations and citation omitted).

In this case, the purported error allegedly rendering the §7203 Orders "void" — the absence of territorial authority to issue the warrant — was made by the Magistrate Judge in the District of Columbia, not law enforcement. Here, both the HSI agent who applied for the search warrant for Monroe's residence, and the Magistrate Judge for the District of Rhode Island who issued that residential warrant, relied in good faith on facially valid Orders issued by the Magistrate Judge for the District of Columbia. Law enforcement agents are not acting unreasonably when, as here, they rely on a facially valid order from a United States Magistrate Judge. See, e.g., Horton, No. 16-3976, 2017 WL 3122073, at *6 (8th Cir. July 24, 2017) ("Further, we have declined to impose an obligation on law enforcement to 'know the legal and jurisdictional limits of a judge's

power to issue interstate search warrants.’’)(quoting *United States v. Houston*, 665 F.3d 991, 996 (8th Cir. 2012)); *United States v. Ammons*, 2016 WL 4926438 at *9 (W.D.KY 2016)(“FBI agents can hardly be faulted for failing to understand the intricacies of the jurisdiction of federal magistrates.”). Accordingly, the good faith exception applies.

CONCLUSION

For the reasons set forth herein, the Defendant’s Motion to Suppress should be denied.

Respectfully submitted,

STEPHEN G. DAMBRUCH
ACTING UNITED STATES ATTORNEY

/s/ John P. McAdams

JOHN P. McADAMS
Assistant U. S. Attorney

CERTIFICATE OF SERVICE

I hereby certify that on this 27th day of July, 2017, I caused the Government's Response to Defendant's Motion To Suppress Evidence be filed electronically and it is available for viewing and downloading from the ECF system.

Electronic Notification:

Olin Thompson, Esq.

/s/ John P. McAdams
John P. McAdams
Assistant U. S. Attorney,
U. S. Attorney's Office
50 Kennedy Plaza, 8th Floor
Providence, RI 02903
401-709-5000, 401-709-5001 (fax)